

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Policies and Rules Governing Interstate Pay-Per-	)	
Call and Other Information Services, and Toll-Free	)	CG Docket No. 04-244
Number Usage	)	
	)	
Truth-in-Billing and Billing Format	)	CC Docket No. 98-170
	)	
Application for Review of Advisory Ruling	)	
Regarding Directly Dialed Calls to International	)	ENF-95-20
Information Services	)	

**COMMENTS OF VERIZON<sup>1</sup>**

The Commission should take prompt action to protect consumers and legitimate long distance carriers from the fraudulent and deceptive practices of information services providers that cause end users to incur international long distance charges that they did not authorize.<sup>2</sup> The problem, known as “modem hijacking,” arises when a customer with dial up access to the internet clicks “I Accept” or “Yes” on certain pop-up ads. As discussed in more detail below, this triggers the downloading of software that reconfigures the customer’s modem to dial international calls, although the customer may not realize it if he or she did not carefully read all the “fine print” of the terms being “accepted.” Calls are then dialed automatically and at random times, without the customer’s knowledge, and are carried by the customer’s presubscribed long distance carrier to international destinations such as Tuvalu, Cook Islands, and Sao Tome. The

---

<sup>1</sup> The Verizon telephone companies and long distance companies (“Verizon”) are the companies affiliated with Verizon Communications Inc. that are listed in Exhibit A to these Comments.

<sup>2</sup> See NPRM, 19 FCC Rcd 13461, ¶¶ 17-18 (2004).

terminating foreign carrier in these locations shares a portion of the international settlement rate it charges to terminate these calls with the scam operator.

To address this problem, the Commission should authorize U.S. international carriers to withhold payment of international settlement rates to foreign carriers that partner with such information service providers. In addition, the Commission should clarify that 47 C.F.R. § 63.19 does not require U.S. international carriers to provide customers notice and to wait 60 days before taking steps to protect consumers and themselves from fraudulent charges by blocking calls to certain numbers or even specific countries when the U.S. international carrier detects significant calling patterns consistent with fraud. Finally, the Commission should work with other U.S. government agencies such as the Federal Trade Commission (FTC) and with foreign regulators, as appropriate, to prosecute these information services providers, and to require them to stop their fraudulent practices and repay victimized consumers.

1. Modem hijacking is a serious problem. Modem hijacking is a significant and growing problem for consumers. The NPRM describes one type of modem hijacking. See NPRM ¶ 17. The type that Verizon and its customers have been experiencing is somewhat different, and works as follows: Typically, a customer using dial-up access to the Internet is presented with a pop-up advertisement or offer.<sup>3</sup> By clicking “I Accept” or “Yes” in the pop-up box, the customer triggers the downloading of software. The software reconfigures the modem to dial international calls. The calls are dialed automatically and at random times without the customer’s knowledge. The disclosure that such software would be downloaded and international calls would be

---

<sup>3</sup> Modem hijacking can also affect a broadband customer if the customer has a dialup line connected to his or her computer (e.g., a line for faxes).

made usually is buried in the “fine print” of the agreement the customer accepts by clicking “I Accept” or “Yes.”<sup>4</sup> The customer, therefore, may not realize what he or she is agreeing to or the rates that will be charged for the international calls.

The international calls generated by the modem are carried over the customer’s presubscribed long distance carrier (such as Verizon Long Distance) to places such as Tuvalu, Cook Islands, and Sao Tome. Verizon Long Distance may carry the calls itself, or may resell the services of another U.S. international carrier, but in either case, Verizon Long Distance cannot distinguish on its network whether a given call is intentionally dialed by an end user or is dialed by downloaded software associated with the scam. The customer may not be aware that these calls are even being made until the charges show up on the customer’s long distance bill. And unless the customer has selected an international discount calling plan, these calls are billed at higher basic international rates.

The scam operators profit by teaming with the terminating foreign carrier in these locations. The terminating foreign carrier charges Verizon or the carrier whose services Verizon resells<sup>5</sup> the international settlement rate to terminate these calls, and then shares a portion of the resulting revenues with the scam operator.

In just the first nine months of 2004, Verizon has handled thousands of complaints by customers relating to this type of Internet dialing scam. This includes over 1,000 complaints to state and federal regulators, the Better Business Bureau, state

---

<sup>4</sup> There have been reports of instances where a consumer triggers the download even if he or she simply attempts to close the pop-up ad. *See, e.g.*, [http://www.fox31news.com/\\_ezpost/data/5147.shtml](http://www.fox31news.com/_ezpost/data/5147.shtml).

<sup>5</sup> In this case, of course, the international settlement rates charged by the terminating foreign carrier are part of the costs the U.S. international carrier considers when determining the rates it will charge Verizon to resell its services.

attorneys general, and Verizon's own Customer Relations Office. The dollar amounts involved in these complaints range from under \$100 to more than \$7,500, with an average of over \$300 per complaint.

2. Verizon has taken steps to protect and educate its customers. Verizon has ongoing efforts to protect customers from these fraudulent scams. For example, Verizon Long Distance has a fraud control group that monitors long distance usage around the clock and looks for unusual usage patterns. If it finds unusual usage patterns, the fraud control group investigates further to assess whether a scam is involved. Verizon also participates in industry-wide groups that share information on scams. If Verizon learns through these or other methods that particular foreign telephone numbers or ranges of numbers are associated with a scam, it will block calls to those numbers. Unfortunately, this is only a temporary fix, as the scammers frequently change their numbers when they realize that calls to their numbers have been blocked.

Verizon also has taken steps to educate its customers and enable them to protect themselves. For example, in April 2004, Verizon issued a press release warning customers about several types of fraud, including modem hijacking, and in August 2004, Verizon issued a press release devoted to advising customers of the dangers of downloading software, and of steps they could take to protect themselves. *See* Attachment 1. Verizon also has placed consumer advisories on a number of its websites.<sup>6</sup>

Despite Verizon's vigilance and efforts, however, it is very difficult to counteract the fraud perpetrated on its customers. For example, as noted above, the scam operators

---

<sup>6</sup> *See, e.g.*, "Beware of Pop-Up Internet Ads and Modem Hijacking" (Aug. 31, 2004) at <http://www.verizon-media.com/iweb/news/20040831.shtml>; "Internet Scam Alert" at [http://www2.verizon.net/announcements/Default.asp?id=modem\\_alert](http://www2.verizon.net/announcements/Default.asp?id=modem_alert); "Internet Modem Switch Scam" at [http://www.vzpacifica.net/consumer\\_advisory.cfm?vzid=1](http://www.vzpacifica.net/consumer_advisory.cfm?vzid=1).

are quick to change numbers when they realize that calls to their numbers have been blocked. In addition, they have begun moving to locations such as Austria and the United Kingdom where there is a significant amount of legitimate international usage, thereby making full country blocking an unworkable solution.

3. The Commission should take prompt action to help protect consumers and legitimate carriers. The Commission and the FTC have recognized that modem hijacking is a serious concern. Both have issued warnings to consumers about these scams. Attachments 2 and 3 to these comments are, respectively, the Commission's Consumer Advisory on Internet Modem Switch Scams from October 2003 and the FTC's Consumer Alert from May 2003. The Commission should go beyond this Advisory and take additional steps to combat this serious problem.

First, the Commission should work with the FTC, other U.S. government agencies, and in cooperation with foreign regulators, as appropriate, to prosecute and shut down scam operators and take action against the carriers that conspire with them or otherwise knowingly accept these arrangements. These entities should be required to disgorge their ill-gotten profits and reimburse the consumers that are their victims.

Second, the Commission should allow U.S. international carriers to withhold payment of settlement rates to foreign carriers in countries with a high incidence of fraud pending Commission review of international charges due to alleged scams. This review could be conducted in response to consumer or carrier complaints or on the Commission's own motion. To the extent these foreign carriers also have been "duped" by the fraud perpetrators, they should be allowed an opportunity to work with affected U.S. carriers to investigate and address the scam. U.S. international carriers should be

permitted to withhold payment of international settlement rates at least until the terminating foreign carrier has identified all of the numbers associated with the scam.<sup>7</sup> If foreign carriers are not willing to cooperate with their U.S. counterparts, U.S. international carriers should be permitted to withhold the international settlement payments until the matter is reviewed by the Commission.

The Commission also should facilitate a joint government-industry review panel, involving affected carriers, consumer groups, and law enforcement, as appropriate. The panel should conduct periodic reviews in order to pursue identified scammers as they change locations, phone numbers, and methods. These reviews could be taken into account in the Commission's own reviews of fraud.

Third, the Commission should make clear that the requirement in Rule 63.19, 47 C.F.R. § 63.19, to provide 60 days prior notice before discontinuing, reducing or impairing service does not apply in the situation where a U.S. international carrier has evidence of fraud and needs to discontinue, reduce, or impair service to certain numbers, ranges of numbers, or destinations in order to prevent fraudulent calls from being made.<sup>8</sup>

---

<sup>7</sup> The Commission also should revise its instructions on filing complaints concerning modem hijacking. Currently, the Commission's website advises consumers filing complaints to include the name of their long distance provider on their complaint. But, as described above, Verizon Long Distance carries these calls because the customer is presubscribed to Verizon Long Distance. Verizon Long Distance is not able to distinguish between calls dialed by end users and those generated by the scam software, yet it incurs the cost of carrying the calls, which includes the charges of the foreign carrier that participates in the scam. The Commission should take the steps described above to target the information services providers and foreign carriers partnering with them that perpetrate this fraud.

<sup>8</sup> The Commission asks whether it should revoke carriers' 214 certification for certain conduct. NPRM ¶ 18. In a scam such as the one described in these comments, legitimate U.S. international carriers are caught in the middle – they simply carry the calls originated on their customers' presubscribed lines and cannot tell whether any given

Finally, the Commission should make available an expedited complaint process for use by U.S. international carriers that seek Commission intervention regarding specific cases of harm to U.S. consumers caused by modem hijacking. For example, the procedure set forth in section 64.1002(d) of the Commission's rules, 47 C.F.R. § 64.1002(d), is designed for swift Commission action pursuant to an expedited schedule of ten days for comments or oppositions and seven days for replies. The Commission could clarify that this expedited complaint process for anticompetitive accounting rates can be used to address these types of fraud, or adopt a similar procedure specifically for the purpose of addressing fraudulent conduct by foreign carriers.

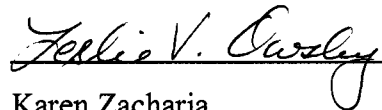
---

call is dialed by an end user or initiated by downloaded software. In either case, however, these carriers incur the cost of carrying the call, including the international settlement rates charged by the foreign terminating carrier that is teaming with the scam operator. Clearly it would not be appropriate to revoke the U.S. international carrier's 214 authority in such situations. If, however, the foreign carrier participating in the scam has a 214 certificate, revocation may be appropriate as one aspect of the solution.

## CONCLUSION

Modem hijacking is a serious and growing problem. The Commission should take prompt action to protect consumers from these fraudulent schemes and to enable legitimate U.S. international carriers to combat these scams.

Respectfully submitted,



Karen Zacharia  
Leslie V. Owsley  
Verizon  
1515 North Court House Road  
Suite 500  
Arlington, Virginia 22201  
(703) 351-3158

Michael E. Glover  
Of Counsel

*Counsel for Verizon*

November 15, 2004



THE VERIZON TELEPHONE COMPANIES

The Verizon telephone companies are the local exchange carriers and long distance companies affiliated with Verizon Communications Inc. These are:

Contel of the South, Inc. d/b/a Verizon Mid-States  
GTE Southwest Incorporated d/b/a Verizon Southwest  
The Micronesian Telecommunications Corporation  
Verizon California Inc.  
Verizon Delaware Inc.  
Verizon Florida Inc.  
Verizon Hawaii Inc.  
Verizon Maryland Inc.  
Verizon New England Inc.  
Verizon New Jersey Inc.  
Verizon New York Inc.  
Verizon North Inc.  
Verizon Northwest Inc.  
Verizon Pennsylvania Inc.  
Verizon South Inc.  
Verizon Virginia Inc.  
Verizon Washington, DC Inc.  
Verizon West Coast Inc.  
Verizon West Virginia Inc.

Bell Atlantic Communications, Inc. d/b/a Verizon Long Distance,  
NYNEX Long Distance Company d/b/a Verizon Enterprise Solutions,  
Verizon Select Services Inc.

# ***NEWS RELEASE***



**FOR IMMEDIATE RELEASE**  
**April 21, 2004**

**Media contacts:**  
**Mark Marchand**  
**518-396-1080**  
**mark.a.marchand@verizon.com**

**Bobbi Henson**  
**972-718-2225**  
**bobbi.henson@verizon.com**

## **Verizon Warns Consumers: Beware of On-Line 'Phishing' Scam**

***Newest Scam Involves Attempts to Collect Credit Card Numbers  
And Other Sensitive Information Through Fake Web Site***

**NEW YORK** – Verizon customers should be aware of a new wave of scams that try to pry personal information from consumers, which can lead to identity theft and other crimes.

The newest scam involves an authentic-looking e-mail from someone posing as a Verizon representative. The e-mail asks Verizon customers to update their personal billing information – such as credit-card or social security numbers -- and directs them to a Web site that is designed to look like a Verizon Web site. The phony Web site is actually operated by the scammers. The e-mail falsely warns the consumer that in order to continue receiving Verizon services, he or she must visit the fake Web site and avoid paying a “processing” fee by updating personal and

account information. Verizon does not do business in this fashion, nor does the company charge consumers to update their information.

This latest wave of scams directing consumers to phony Web sites -- known as "phishing" -- has targeted a number of other industries and companies over the past year.

"Consumers should be wary of any e-mail or phone call asking that they reveal credit card or other sensitive information," said Jim Trainor, Verizon vice president-security. "Verizon customers can call us via the phone number on their bills, or they can visit our real home page -- [www.verizon.com](http://www.verizon.com) or our Verizon Online home page, [www.verizon.net](http://www.verizon.net) -- if they have any suspicions about an e-mail, phone call or letter.

"The bottom line is there are many scam artists out there willing to do anything to trick consumers into giving up personal information or money," Trainor said. "Take the extra step and ask a question or call us if you have any doubt at all."

### **Other Scams Also Threaten Consumers**

In issuing its warning about "phishing," Verizon also made consumers aware of several other scams:

- **Pop-up ad questions** – This is another relatively new issue. Verizon Online customers and other Internet access-provider consumers should carefully scrutinize what they agree to when they click on Web site pop-up ads and are asked to respond to a series of questions. In some cases, dial-up consumers who clicked "yes" to several pop-up ad questions have found their computer modems re-programmed to make expensive long-distance calls. Pop-up ads are a legitimate way of advertising on Web sites – but consumers should read the fine print and make sure they know what they're agreeing to when they click the "yes" button in response to questions in such an ad. It could be a costly mistake.
- **Collect calls from unknown callers** – This is a relatively old scam that has been surfacing again recently in several areas of the country. Under this scam, a caller –

sometimes an inmate from a correctional facility – calls people through an operator and asks them to accept a collect call by convincing them someone they know is in jail. In the relatively rare circumstances where the called party accepts the call and associated charges, the caller hangs up and the consumer is stuck with a charge for the collect call. In some cases, the scammer stays on and tries to convince the consumer to program his or her incoming calls to be forwarded to another destination. In some cases, this can then lead to the scam artist making additional long-distance calls that are then charged to the unsuspecting consumer. The bottom line is: Never accept a collect call unless it is from someone you know or from someone whose identity you can verify.

- **Callers or letter-writers masquerading as Verizon employees** – Verizon has seen many different variations on this scam over the years, but the overall purpose remains the same: trick an unsuspecting consumer into giving up personal information that can be used to commit identity theft or other crimes. In one variation of this scenario, the caller identifies himself as a Verizon representative and says the consumer in his or her most recent payment to Verizon paid more than the balance due. In order to process a refund check, the scammer says, the customer should provide some personal information that can be used to speed the processing of the check. Again, Verizon does not do business in this fashion. Any overpayments are automatically credited to the next month's bill – without Verizon having to contact the consumer or the customer having to call Verizon. In general, if you receive such a phone call, ask the caller for a callback number or simply hang up and call Verizon via the business office phone number listed on your bill.

“By simply taking that one extra minute to consider whether something is a legitimate communication from a trusted source, consumers can save themselves both a lot of headaches and maybe a lot of money,” Trainor said. “Usually just one extra question or taking a minute to check out an e-mail or online ad is enough for a consumer to stop the scammers dead in their tracks.”

A Fortune 20 company, Verizon Communications (NYSE:VZ) is one of the world's leading providers of communications services, with approximately \$68 billion in annual revenues. Verizon companies are the largest providers of wireline and wireless communications in the United States. Verizon is also the largest directory publisher in the world, as measured by directory titles and circulation. Verizon's international presence includes wireline and wireless communications operations and investments, primarily in the Americas and Europe. For more information, visit [www.verizon.com](http://www.verizon.com).

####

VERIZON'S ONLINE NEWS CENTER: Verizon news releases, executive speeches and biographies, media contacts and other information are available at Verizon's News Center on the World Wide Web at [www.verizon.com/news](http://www.verizon.com/news). To receive news releases by e-mail, visit the News Center and register for customized automatic delivery of Verizon news releases.

# ***NEWS RELEASE***



**FOR IMMEDIATE RELEASE**  
**August 30, 2004**

**Media contact:**  
**Ells Edwards**  
**302-576-5340**  
[ellsworth.edwards@verizon.com](mailto:ellsworth.edwards@verizon.com)

## **Verizon Issues Consumer Alert: Beware of Pop-Up Internet Ads and ‘Modem Hijacking’ Scheme**

***Consumers Who Click ‘yes’ to Pop-Up Ad Questions Without Reading The Fine Print Could Be Agreeing to Have Their Modems Programmed to Automatically Dial Expensive International Long-Distance Calls***

**NEW YORK** – Consumers should read the fine print before clicking “yes” or “I accept” to questions that appear on so-called pop-up ads while browsing the Web. They could be agreeing to install software on their computers that then dials international locations. The result could be significant, and perhaps unexpected, international long-distance charges for which the customer is responsible.

This scam, known as “modem hijacking,” occurs when a computer user sees certain ads pop up on the screen while visiting a Web site. If the user clicks on the pop-up, a series of questions appears asking the user to choose a “yes,” “I agree,” or a similarly phrased button to agree to the terms and conditions of the ad. A positive response to the question triggers a

software download to the user's computer – which will then automatically dial the international phone numbers at random times without the customer knowing it.

The Federal Trade Commission, in response to increasing incidents involving this scam, has posted a consumer alert on its website at:

<http://www.ftc.gov/bcp/online/pubs/alert/modmalrt.htm>.

Consumers should always carefully read the disclosures, terms and conditions before agreeing to questions in on-line ads or permitting software to be installed on their computer.

John Broten, president of Verizon Long Distance advises: "If you have any doubt, do not agree to the download. If you do, you are essentially allowing someone, unknown to you, to use your computer. This may generate significant long-distance charges that you will be responsible for paying."

The ads associated with the scam often promise entertainment for free, which Broten notes, "should be a warning to consumers, since there is no such thing as a free lunch." The scam is primarily aimed at dial-up Internet users, not those who use a broadband connection such as DSL or cable modems. However, a word of caution to broadband users: If you still have a telephone line connected to your modem – to send faxes, for example – you are still vulnerable to this scam.

Internet access account owners in a household or business should make sure that all family members and others who might use the computer are aware of the potential scam.

Customers can take preemptive action to better protect themselves from these scams and unexpected charges that may result.

Here are the key points to consider:

- Carefully read all the terms and conditions of any offer before downloading anything to your computer; unless you fully understand everything you are agreeing to, do not accept the download.
- Contact a reputable software vendor about programs that block pop-up ads ("pop-up blockers"), and identify and remove the types of programs that may be associated with modem-hijacking scams.
- Disconnect the telephone line to your modem when it is not in use.

A Dow 30 company, Verizon Communications (NYSE:VZ) is one of the world's leading providers of communications services, with approximately \$68 billion in annual revenues. Verizon companies are the largest providers of wireline and wireless communications in the United States. Verizon is also the largest directory publisher in the world, as measured by directory titles and circulation. Verizon's international presence includes wireline and wireless communications operations and investments, primarily in the Americas and Europe. For more information, visit [www.verizon.com](http://www.verizon.com).

#####

VERIZON'S ONLINE NEWS CENTER: Verizon news releases, executive speeches and biographies, media contacts and other information are available at Verizon's News Center on the World Wide Web at [www.verizon.com/news](http://www.verizon.com/news). To receive news releases by e-mail, visit the News Center and register for customized automatic delivery of Verizon news releases.



**Consumer & Governmental Affairs Bureau**[FCC](#) > [CGB Home](#) > [Consumer Info Directory](#) > [Modem Switch Scam](#)[FCC site map](#)

# Consumer Advisory

## Internet Modem Switch Scam

Consumers have informed the Federal Communications Commission (FCC) that they have been billed for international calls that occurred as a result of using local (domestic) Internet service providers to access Web sites. The FCC wants you to know that we are monitoring the situation and that there are some precautions you can take to minimize your chances of becoming a victim.

### Here's How It Works

Some Web sites encourage computer users to download software in order to view certain material. Unknown to that user, the downloaded software disconnects his or her computer's modem and then reconnects it using an international long distance number. The result: the modem may actually be placing a call to as far away as Chad, Madagascar or other countries, and the computer user may be billed for an international call.

**IMPORTANT:** Don't download programs from the Internet without reading the disclosures. Some Web sites may be advertised as "free and uncensored" or may allow information to be downloaded. However, a pop-up window with a disclaimer should appear. The disclaimer usually reveals information on possible charges or the rerouting of the Web site. It may say, "you will be disconnected from your local Internet access number and reconnected to an international location" (which may be Chad, Madagascar, or Vanuatu). It is important that consumers read the disclaimer to learn what charges will be assessed before they click the box. If they still choose to download, consumers should be prepared to receive a phone bill with high international toll charges. There may also be charges from a non-telecommunications company that provides a billing service to the Web site in question.

To minimize the risk of this happening, consumers should get from the local phone company an INTERNATIONAL BLOCK on their computer line.

### Filing a Complaint with the FCC

There is no charge to file an informal complaint with the FCC. Your complaint letter should include your name, address, telephone number or numbers involved with your complaint,

## Attachment 2

a telephone number where you can be reached during the business day, and the name of your long distance carrier. Your letter should also provide as much specific information about your complaint as possible, such as an explanation of the circumstances possible, such as an explanation of the circumstances that led to your complaint, the names of all telephone or other companies involved with your complaint, the names and telephone numbers of the telephone company employees that you talked with in an effort to resolve your complaint, the dates that you talked with these employees, and any other information that would help the FCC to process your complaint. Your local telephone company also often has records that are essential to processing your complaint. You should then mail your complaint to:

Federal Communications Commission  
Consumer & Governmental Affairs Bureau  
Consumer Inquiries and Complaints Division  
445 12th Street, SW  
Washington, DC 20554

To file your complaint electronically, go to: [www.fcc.gov/cgb/complaints.html](http://www.fcc.gov/cgb/complaints.html). You can also file by e-mail at: [fccinfo@fcc.gov](mailto:fccinfo@fcc.gov).

**Filing a Complaint with the Federal Trade Commission (FTC)**

You can also submit your complaint, in writing, to the FTC. The FTC does not typically investigate or resolve specific complaints, however, but rather looks for trends or patterns when an issue appears to warrant action. Your FTC complaint should be mailed to:

Consumer Response Center  
Federal Trade Commission  
600 Pennsylvania Ave., NW  
Washington, DC 20580

FTC toll-free number: 1-877-382-4357  
FTC email address for reporting fraud: [crc@ftc.gov](mailto:crc@ftc.gov)

*For this or any other consumer publication in an accessible format (electronic ASCII text, Braille, large print, or audio) please write or call us at the address or phone number below, or send an e-mail to [FCC504@fcc.gov](mailto:FCC504@fcc.gov).*

*To receive information on this and other FCC consumer topics through the Commission's electronic subscriber service, click on [www.fcc.gov/cgb/emailservice.html](http://www.fcc.gov/cgb/emailservice.html).*

*This document is for consumer education purposes only and is not intended to affect any proceeding or cases involving this subject matter or related issues.*

*last reviewed/updated on 10/06/03*

[FCC Home](#) | [Search](#) | [Updates](#) | [E-Filing](#) | [Initiatives](#) | [For Consumers](#) | [Find People](#)

# FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and Business Education

## When Your Computer Makes A Call... Without Your Okay

If you use the Internet, you're probably dialing a local phone number to get online. Chances are you know exactly what you pay for that local service. However, many consumers are surprised to find they've been charged for calls to destinations that aren't remotely local, simply *remote*. The calls were made through their modems without their knowledge or approval.

How does it happen? According to the Federal Trade Commission (FTC), the nation's consumer protection agency, it's a scheme some Web sites use to trick consumers into paying to access "free" Internet content. Often, the sites claim to be "free" or advertise that "no credit card is needed," then prompt the user to download a "viewer" or "dialer" program. Here's the catch: Once the program is downloaded to the user's computer, it disconnects from the Internet and reconnects using another phone number — a domestic long distance, international or 900 number — at rates between \$2 and \$7 a minute.

The FTC says these scams, which are typically associated with adult sites, don't require a credit card number for access. That means they're available to children, who can click onto them without their parents' knowledge or permission. Even if parents disable international calling from their phone lines, many modem dialers are programmed to circumvent the "block," and initiate international calls using a "10-10 dial-around" prefix.

Here's how you can minimize your chances of finding surprise charges on your phone bill:

- Consider a dedicated phone line for your computer and restrict it to local calls.
- Pay attention to any program that enables your modem to re-dial to the Internet. If you see a dialog box on your computer indicating that it's dialing when you didn't direct it to, cancel the connection and hang up. Check the number you're dialing and continue only if it's a local call.
- Make sure your modem makes an audible noise when dialing a phone number — so you can hear that a new connection is being made.
- Delete any dialer programs that have been downloaded onto your computer.
- Read online disclosures carefully. They may be buried several clicks away in pages of small print. In addition, read the language in the typical gray boxes on your screen. Don't click on "OK" unless you know exactly what you're agreeing to.

- If in the past you used a modem to dial up the Internet and now you use a high-speed DSL or cable connection, disconnect the phone line from your computer. You don't need it to access the Internet any more, and it could leave you vulnerable to a dialer program.
- You may want to install a firewall, especially if you use a high-speed Internet connection. A firewall is software or hardware designed to block hackers from accessing your computer. You also might consider increasing the security settings on the operating system software on your computer.
- Talk to your children. Explain that they could be targets of international modem dialing scams and tell them the consequences of downloading "viewer" or "dialer" programs on the computer.
- Monitor your children's Internet use. Keep track of the Web sites your children visit by checking the Web browser history files and cache.
- Be skeptical when surfing the Web especially when you see claims like "free" or "no credit card needed" in exchange for a product or service.
- Dispute the charges with the company doing the billing.
- Save the bill. If you think you've been a victim of unauthorized modem dialing, it may help identify the scammers when you report the incident.
- Take action if you are billed for access to Internet content that you didn't authorize. Use the complaint form at [www.ftc.gov](http://www.ftc.gov), or contact the FTC, toll-free, at 1-877-FTC-HELP (1-877-382-4357).

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit [www.ftc.gov](http://www.ftc.gov) or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.



May 2003